PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-244495
(43)Date of publication of application : 08.09.2000

(51)Int.Cl. H04L 12/24
H04L 12/26
H04L 12/56

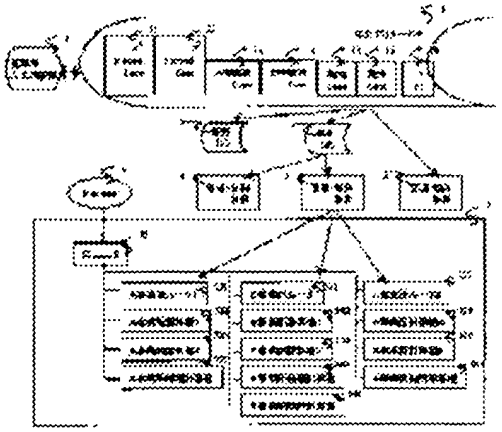
(21)Application number : 11-044134
(22)Date of filing : 23.02.1999

(71)Applicant : HITACHI LTD
(72)Inventor : YOSHIDA KENICHI
MIYAKE SHIGERU
HIRATA TOSHIAKI
KOIZUMI MINORU
TAKADA OSAMU

(54) NETWORK MANAGING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To easily execute necessary setting by setting an operation policy stored in a data base to be the description of a job content executed in a unit constituting a network and converting the description of the job content into control information on the unit constituting the network based on an appropriate processing.



SOLUTION: An operation policy stored in a data base is the description of a job content executed in a unit constituting a network and the description of the job content is converted into control information on the unit constituting the network based on an appropriate processing. A company network which is formed of two offices and accounting section/industry section managing the two offices and which uses TCP/IP technology is assumed for the network 5 of a management object. Center policy DB1 stores the operation policy of the network 5 and is constructed on a general computer. A management controller 3 supports the transmission of data between center policy DB1 and the unit constituting the network 5 in the middle of them.

LEGAL STATUS

[Date of request for examination]	17.01.2003
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3659052
[Date of registration]	25.03.2005
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The network management system which the employment policy memorized by this database is description of the work breakdown performed by the device which constitutes this network, and is characterized by to be changed into the control information of the device which constitutes a network based on processing with appropriate description of this work breakdown in the network management system which consists of a database which memorizes the employment policy of the network which consists of a router, a calculating machine, etc., and this network.
[Claim 2] The network management system characterized by having supervisory control equipment which supports both signal transduction in a network management system in the medium of this database and the device which constitutes this network in the publication of claim 1.
[Claim 3] The network management system characterized by having the duplicate database of this database in the publication of claim 1 in a network management system.
[Claim 4] The network management system with which description of this work breakdown is characterized by being the operation which the user group using a ** network takes charge of in a network management system claim 1 thru/or given [any 1] in three.
[Claim 5] The network management system characterized by being description about the application program performed on the computer by which description of this work breakdown was connected to the ** network in a network management system claim 1 thru/or given [any 1] in three.
[Claim 6] The network management system with which description about this user group's operation in its duty is characterized by including the information about this user program that carries out a user group activity, and the information about the user group with whom this user program communicates in a network management system according to claim 4.
[Claim 7] The network management system characterized by the description about this application program including the information about the communications protocol which this application program uses, and the information about a communication link place in a network management system according to claim 5.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the network management system and management method for offering the structure which sets up access list, QoS setting out, VPN setting out, etc. of a large-scale network simply while consisting of subnets in which many management policies differ from two or more routers or Firewall equipment especially with respect to a computer network.
[0002]
[Description of the Prior Art] In the large-scale network while consisting of subnets in which many management policies differ from two or more routers or Firewall equipment conventionally, the content of setting out of each router or Firewall equipment was remarkable, and it was complicated. For example, RFC2401 etc. took the technical force advanced for understanding these to a security-related technique, such as VPN (Virtual Private Network), although, as for the QoS (Quality of Service)-related technique, specification was described by RFC2205 etc. Moreover, in relation to these specification, the approach of carrying out automatic distribution of the setting out from a remote place point is also devised (for example, draft-ietf-rap-cops-05.txt of Internet Draft etc.). However, it is the same at the point of needing network instrument setup information.
[0003]
[Problem(s) to be Solved by the Invention] For this reason, important setting out or important setting out of QoS were not fully released off lack of an expert with an advanced know how in the conventional network administration on security like an access list or VPN. This invention solves the above-mentioned technical problem, and aims at offering the network management system which can perform required setting out simple, and a management method. Moreover, it aims at offering the software which realizes the above-mentioned managerial system and a management method and which is used for each computer.
[0004]
[Means for Solving the Problem] In order to attain the above-mentioned object, this invention offers the structure which generates automatically and sets up setting out of each router, Firewall equipment, etc. from the definition about the operation performed on a network. This structure enables it to perform complicated network administration simply by the conventional approach. Namely, in addition to an expert like an access list or VPN, required setting out can be performed now simple by carrying out automatic conversion of the difficult setting out of setting out from a work breakdown intelligible for a user.
[0005]
[Embodiment of the Invention] Hereafter, one example of this invention is explained to a detail. Drawing 1 is drawing having shown the example of a configuration of the network which applied this invention. In drawing 1, 5 is the network of an administration object and assumes the network in an enterprise using the TCP/IP technique which consists of an accounting department and a labor division which manages two places of business and both places of business here. 1 is the central policy DB

which memorizes the employment policy of a network 5, and is the database built on the common calculating machine. 11, 12, 13, 14, 15, 16, and 17 are the examples of the content of storage of the central policy DB1, and 11-16 are what described the example of operation which the user group using a network 5 takes charge of, and show the example of a content to drawing 2. 17 is description about the application program performed on the computer connected to the network 5, and shows the example of a content to drawing 3. 2 is the duplicate DB which copied the content of the central policy DB1, and is good in the suitable database on a calculating machine. 3 is supervisory control equipment which supports both signal transduction in the medium of the device which constitutes the central policy DB1 and a network 5, and is good by the common computer possessing a suitable program. 4 is an administrative I/O device for displaying and correcting the content of the central policy DB1, and is good at the I/O device of a suitable computer.

[0006] A network 5 is constituted from a computer 532, 533, 535, 536, 538, 539, 542, 543, 545,546 and a router 531, 541, and 537 by drawing 1, and it connects with Internet 6 through the firewall 52. Among these, a router 531 and 537 A computer 532, 533, 535, 536, 538, and 539 are the routers and computers of A place of business, and are a router 541. A computer 542, 543, 545, and 546 are the routers and computers of B place of business. Moreover, a computer 535 and 545 belong also to an accounting department, and a computer 536 and 546 belong also to the labor division.

[0007] Becoming important when managing intranet like a network 5 sets up a firewall 52 correctly, and it is [that a crack is only made not to be carried out and] from the outside. The work breakdown of an accounting department or a labor division has much information to which secrecy nature should be kept in in the company. Moreover, there may be information mutually made into secrecy also between places of business. In such a case, it is necessary to set a network device as the appearance to which the access control by VPN or the router is performed, and unnecessary information transfer is not performed. moreover, operation -- depending on an application, the communication link quality of a large quantity and a high speed is needed, and QoS control should be performed With the conventional technique, the manager of a network 5 needed to set up the access list and VPN of a router 531, 541, and 537 grades so that the above-mentioned demand might be filled. However, setting out of VPN or QoS was complicated, and also when sufficient setting out was not made from lack of an expert, there was. Below by this invention, the demand from the above operation explains that it can generate automatically to network instrument setup information, such as a router.

[0008] Drawing 2 is the example of a content of the Zone definition memorized by the central policy DB. By this example, Zone means the user group using a network. Description concerning [the Zone definition illustrated by drawing 2] this user group's operation in its duty is the information about this user program that carries out a user group activity, and the information about the user group with whom this user program communicates. The example of a content of drawing 2 is specifically an example of description for every operation group about the application program performed on the computer which was memorized by the central policy DB1, and which was connected to the network 5. The definition of the application program with which 111 are performed in Internet relation among drawing 2, The definition of the application program with which 121 is performed in FireWall relation, The definition of the application program with which 131 is performed in A place-of-business relation, The definition of the application program with which 141 is performed in B place-of-business relation, The definition of the application program with which 151 is performed in accounting relation, and 161 are the definitions of the application program performed in labor relation, and the name and communication link place of a user program are specified, respectively.

[0009] By Internet Zone, as for drawing 2 and 111, Electrons mail (1111), news (1112), and WWW (1113) and telnet (1114) communicate between FireWall Zone as an application program, among these, as for Electron mail, what a communication link is preferentially processed for (inside of 1111 and a priority) is specified. Moreover, what (1114) telnet forbids communications processing other than Firewall for clearly is specified. This assignment is changed into setting out against explicit access in a router by the below-mentioned algorithm. The line (1115) of the further 111 last specifies that applications other than the above communicate with Internet Zone. as for drawing 2 and 121, news

(1212)/telnet (1215) communicates among all Zone(s) by Electron mail communicating in all Zone(s) and priorities as an application program in FireWall Zone (1211), and WWW communicates only between Internet Zone -- having (1213) -- WWW proxy specifies what is communicated between A and B place of business (1214).

[0010] Drawing 2 and 131 specify what (1314) Electrons mail (1311), news (1312), and WWW proxy (1313) communicate with Firewall Zone, and telnet communicates with FireWall Zone and B place of business, and the thing which the user program which uses port numbers 4096 and 4097 communicates between B places of business (1315 and 1316) in A place of business. Moreover, Telnet, the port number 4096, and the user program that uses 4097 are clearly forbidden from performing a communication link with Internet Zone. Moreover, it specifies carrying out data communication of the user program of a port number 4096 preferentially in priority size (1314, 1315, and 1316).

[0011] Although drawing 2 and 141 are the definitions of B place of business and are the same as that of the definition of A place of business, about telnet, utilization between FireWall Zone is also forbidden only between A places of business (1414). drawing 2 and 151 -- an accounting-related definition -- accounting-related operation -- electrons mail (1511), WWW proxy (1512), and telnet (1513) the user program of port numbers 5001-5003 -- it is (1514, 1515, and 1516) -- it is only the communication link inside accounting Zone, and the communication link with its other post is forbidden. Drawing 2 and 161 are the definitions for the labor related operation groups who restricted the communication link to Labor Zone similarly.

[0012] Drawing 3 is the example of a definition of the information about the communications protocol which the application program memorized by the central policy DB uses, and the information about a communication link place, and calls AP definition below. Drawing 3 and 171 are definitions independent [user-program AP1]. AP1 is performed from the program AP 171 performed by the computer of the A place of business Zone, and two subprograms of AP172 of A place of business performed only especially by the computer 2. Moreover, that AP171 communicates by the computer 1 and port number 1111 of B place of business by the computer 2 and port number 1112 of (1711) and B place of business (1712), that AP172 communicates by the computer 2 and port number 1113 of B place of business by the computer 1 and port number 1114 of (1713) and B place of business (1714), and communicating by the computer and port number 1115 of arbitration of A place of business (1715) are specified.

[0013] Drawing 2 and the content of storage of the central policy DB1 explained using 3 are the examples which summarized setting out of a communication link required for the operation performed in an enterprise, and setting out against [for security maintenance] a communication link by the tabular format above. Drawing 2 is an example of a definition about the operation of the place of business which is an organization in a firm, and drawing 3 is an example of a definition about the application program used in a firm.

[0014] The network administration by this invention sets up automatically the equipment which constitutes a network based on the above information. At this time, it is also possible to express the above information graphically to administrative I/O device 4 etc. Drawing 4 is the graphical example of a display of the Zone definition corresponding to drawing 2. Drawing 5 is the example of a display of AP definition corresponding to drawing 3. Moreover, drawing 6 R> 6 is the example of a display of only the information on telnet (1114, 1215, 1314, 1414, 1513, 1513, and 1613) among the information on drawing 2 . Notice these about it being the content same as information about a network management policy. For example, after drawing 4 displays the box corresponding to Zone on the suitable location on a screen, if it changes a line type and the information on the communication link place for every application classification is displayed as a line, it is generable from drawing 2. At this time, if the information against a communication link puts x mark on a line, it can be displayed. When the drawing which added the information against a communication link to drawing 4 is considered, conversion to drawing 2 is also easy.

[0015] The manager who manages a network by this invention is correcting the content of the central policy DB1 through administrative I/O device 4, and manages a network. In this case, the content of the

central policy DB1 may be corrected by correcting the information on drawing 2 and a tabular format like 3, and drawing 4 and a graphical display like 5 and 6 may be corrected using the editor ability for graphic forms.

[0016] Drawing 7 is the example of a definition of the extra information memorized by the central policy DB1. In the managerial system of the network by this invention, the physical configuration information of a network 5 other than a network employment policy is memorized of the central policy DB1. Drawing 7 and 100 are the examples of a router definition, and 101 is the example of a VPN definition. To drawing 7 and 100, the router (1001) of a name called router1 FireWall Zone and IP address 192.10.0.1, it is connected with the interface of a subnet mask 255.255.0.0 (1003). A place of business and IP address 192.11.0.1, it is connected with the interface of a subnet mask 255.255.0.0 (1004). B place of business and IP address 192.12.0.1, it is connected with the interface of a subnet mask 255.255.0.0 (1005). It is IP address 192.13.0.1 to another site (for example, office in the location locally left although it was the place of business same on a company organization) of A place of business, What is connected with the interface of a subnet mask 255.255.0.0 (1006) is described. Moreover, memorizing the initialization file of router generated using drawing 2 and 3 or 7 information to a file called X1 is specified (1002).

[0017] It specifies that drawing 7 and 101 use the virtual network (VPN: Virtual Private Network) technique which used the encryption communication link and the authentication technique for security reservation in order to carry out accounting operation. The name of this virtual network is specifically VPN1 (1011). The IP addresses of the machine which participates are 192.11.0.10 (equivalent to A place-of-business accounting computer 535 at drawing 1), and 192.12.0.10 (equivalent to B place-of-business accounting computer 545 at drawing 1) (1012). The initialization files generated to each machines are X192.11.0.10 and X192.12.10.10, respectively (1013), In order to send using Y1 as a cipher system (1014), using Y2 as an authentication method (1015), and required data, it specifies using a port number 5000 (1016).

[0018] Drawing 8 and 302 are drawing 2 and the setting-out information for interface 1 of router1 made from 3 or 7 information. The information (3021) on the interface address and a subnet is created from the information (1004) on drawing 7 by drawing 8. The information on the access permission and disapproval not more than it is generated from drawing 2 and the information on 3. (The creation approach is later mentioned using drawing 12) . Setting out (3022) to which the communication link with 192.13.0.0/255.255.0.0 is permitted about all the port numbers to begin means permitting all communication links from another location of the same place of business. The access permissions (3023) of the following port numbers 1111-1114 are drawing 3 and setting out corresponding to 171. Setting out (3024) of the following port numbers 23 (telnet)-4097 is setting out corresponding to drawing 2 and prohibition of the communication link of 131. Setting out (3025) of the following port number 5000 is setting out corresponding to drawing 7 and VPN setting out of 101. Setting out (3026) of the following port numbers 25-23 is setting out corresponding to drawing 2, the electrons mail (25), news (119), and WWW proxy of 131 (8080), and the communication link assignment with FireWall Zone of telnet (23). The following port numbers 23-4097 are setting out (3027) corresponding to the communication link assignment with drawing 2 and B place of business of 131.

[0019] Drawing 8 and the last access disapproval (3028) are setting out for not permitting a communication link except the above setting out. As for the example of setting-out information illustrated to drawing 8, the information on the access permission and disapproval of a router assumes that actual access is controlled by assignment of the authorization and the disapproval of access that check in order and conditions were fulfilled first. Since the information on 302 is checked sequentially from a top, assignment of the last access disapproval becomes the semantics of disapproval altogether except the above-mentioned setting out.

[0020] The information on a priority is changed from the information on drawing 2 and the priority of 3 by drawing 8. The structure of QoS changes with activities of the hardware of a router. Drawing 2 and the priority of 3 are assignment of a due to occupational cases priority, and the information on the priority of drawing 8 is assignment of the changed priority that the structure of QoS which router

hardware supports was followed. In the case of this example, it assumes transposing assignment of size, inside, and smallness to priority simply. Drawing 8 and 303 are the setting-out information on VPN made from drawing 2, the information on 151, and drawing 7 and the information on 101. VPN-related setting-out information is the information from drawing 7, and the information on an access permission is drawing 2 and the information from 151.

[0021] Conventionally, after he was conscious of drawing 2 and the employment policy of the network illustrated to 3, the network operations manager had set up manually setting out of the router illustrated to drawing 8, and VPN. However, the know how was needed for such setting out, and it was not able to do simply. Moreover, according to the work breakdown, the way of thinking of describing an employment policy was not common, either, drawing 2 and the database itself illustrated to 3 were not maintained on the computer, and the attempt of automatic creation of setting out illustrated to drawing 8 was not successful. In this example, the algorithm later mentioned using drawing 12 generates the information on drawing 8 from drawing 2 and 3 or 7 information.

[0022] It is the database formed in order for duplicate DB2 to distribute the load of the central policy DB1 in large-scale network configuration in this example. In a network management policy, it refers to the real time, and a problem may arise in the usual database system at the response time etc. Management and a control unit 3 are equipment formed for the object, such as improvement in the response time, and has the information which changed into setting out (it illustrates to drawing 8) of a router (it illustrates to drawing 2 and 3) the content memorized of the central policy DB, and the information for modification of setting-out information in supervisory control equipment 3 in this example for the improvement in a speed of response. Conversion to the information illustrated to drawing 8 from drawing 2 and the information illustrated to 3 and 7 may be performed by the central policy DB1. Moreover, you may carry out by duplicate DB2 and management and a control unit 3 may perform. Hereafter, suppose that it changes with supervisory control equipment 3 in this example.

[0023] The information on drawing 8 generated in this example assumes the configuration file only once [of the start] to set it as a network device manually. Setting-out modification of the 2nd henceforth is automatable. drawing 9 -- therefore, the example of the content of storage memorized to supervisory control equipment 3 is shown. 300 is the example of the data for router control of the supervisory control equipment 3 interior in drawing 9, and 301 is the example of the data for VPN control of the supervisory control equipment 3 interior. Drawing 9 and the content of storage illustrated to 300 are the interface information (3003, 3004, 3005, and 3006) and the control-system (3007) authentication approaches (3008) of a router required in order to set router1 as 2nd henceforth from the outside. When using this information and drawing 2 and the content of 3 and 7 are changed, the supervisory control equipment 3 which received the changed content of drawing 8 can change setting out of the interface specified as insurance by encryption communication link, after attesting to a router according to the specified authentication approach. Specifically, the object with the same information on drawing 9 is manually set as network devices, such as a router, with the information on drawing 8 only once [of the start]. Since the information about the control / authentication method with same supervisory control equipment 3, router, etc. is sharable by this, supervisory control equipment 3 makes control / setting-out change of the router etc. via a network. Drawing 9 and 301 are the examples of information which supervisory control equipment should have in VPN setting-out modification similarly.

[0024] Drawing 10 is the example of the data communication protocol used between the central policy DB1, duplicate DB2, and management and a control device 3. The protocol of the arbitration suitable for the duplicate of a database should just be used between the central policy DB1 and duplicate DB2. Between management and a control unit, and a router, when there is a limit on mounting of a router, utilization of a simple protocol like SNMP, and the protocol suitable for renewal of dynamic like COPS and a protocol like LDAP can be considered. A protocol like HTTP can also be used between the central policy DB1, or duplicate DB2, and management and a control unit 3.

[0025] Drawing 11 is an example of data flow in case supervisory control equipment 3 generates setting-out information. What is necessary is just to merge a result finally independently, respectively, although automatic generation is considered by this example for setting out of the interface information on a

router (72), an access list (73), QoS (74), and VPN (75) (76). Drawing 8 and 302 have brought the result of having merged interface information and the information on an access control.
[0026] Drawing 12 is an example of an algorithm in case supervisory control equipment 3 generates the setting-out information on an access permission and disapproval relation in the processing 73 of the algorithm illustrated to drawing 11. Hereafter, actuation of drawing 12 is explained to an example for the generation process of access related setting out illustrated to drawing 8. In drawing 12, access related setting out of drawing 8 is generated sequentially from the bottom. For this reason, the access disapproval definition of all services (port number) is first defined as a content of the access control list (81). Thereby, setting out (3028) of drawing 8 and the last access disapproval is generable. Next, the existence of the service whose access permission has been processed is investigated in drawing 2, and authorization setting out of access to (82) and its service is generated (83). Setting out (3026) of the port numbers 25-23 corresponding to setting out (3027) of the port numbers 23-4096 corresponding to the communication link assignment with drawing 2, telnet (23) of 131, 4096, and B place of business of 4097, and drawing 2 on it, the electrons mail (25), news (119), and WWW proxy of 131 (8080) and the communication link assignment with FireWall Zone of telnet (23) is generated by this processing. The access permission (3025) of the port of No. 5000 is also outputted here. This is generated by retrieving the information on the port number which VPN uses, and the computer which has participated to the VPN from drawing 7 and the information on 101.
[0027] Next, the existence of the service whose access disapproval has been processed is investigated in drawing 2, and disapproval setting out of access to (84) and its service is generated (85). Setting out (3024) of drawing 2 and the access disapproval of the port numbers 23 (telnet)-4097 corresponding to prohibition of the communication link of 131 is generated by this processing. next, the processed operation of access information -- (87) which investigates the existence of an application and adds the definition of an access permission to (86) and its operation AP to the head of an access list. Setting out (3023) of the access permission of drawing 3 and the port numbers 1111-1114 corresponding to 171 is generated by this processing. From another location of the same place of business, all communication links are permitted at the end (88). Setting out (3022) of communication link authorization with 192.13.0.0/255.255.0.0 is generated about all port numbers by this processing.
[0028] The information on the priority of drawing 8 is convertible from the information on drawing 2 and the priority of 3 in process of the above. Although the structure of QoS changes with activities of the hardware of a router as mentioned above, if it carries out easy [of the conversion table for changing assignment of drawing 2 and the priority of 3 into the information on the priority of drawing 8], when generating an access list in process of the above, the information on a priority can also be changed simultaneously. The central policy DB1 and duplicate DB2 are good in the suitable database constituted on a common calculating machine. Moreover, supervisory control equipment 3 is also good by the common computer possessing the suitable soft ware. The example of a configuration of the computer which fitted drawing 13 at these is shown. The computer 900 illustrated to drawing 13 is the thing of a general configuration, and consists of main storage 901, a central processing unit 902, a network control unit 903, a display control 905, a disk controller 907, and a disk unit 906. What is necessary is just to connect a display 8 and Local Area Network 904 to a computer 900 as an external device.
[0029] When using this computer 900 as a computer which builds the central policy DB1 or duplicate DB2 on it, drawing 2 and the data illustrated to 3 and 7 are memorized by the database on a disk unit 906. This database is controlled by the suitable database software which is memorized on main storage 901 and processed with a central processing unit 902. Moreover, when using this calculating machine 900 as supervisory control equipment 3, drawing 8 and the data illustrated to 9 are memorized by the database on a disk unit 906. This database is controlled by the suitable database software which is memorized on main storage 901 and processed with a central processing unit 902. Moreover, drawing 11 and processing illustrated to 12 are performed with the suitable software which is memorized on main storage 901 and processed with a central processing unit 902.
[0030] In the above example, the example of a definition about the operation of the place of business which is an organization in a firm, and the example of a definition about the application program used in

a firm were memorized of the central policy DB1. Both these may be memorized of the central policy DB1, and either may be memorized of it. Moreover, although network physical configuration information was memorized together of the same central policy DB1, what is memorized in another database is sufficient. The content of storage of the central policy DB1 may be corrected by correcting the information on drawing 2 and a tabular format like 3, and may correct drawing 4 and a graphical display like 5 and 6 using the editor ability for graphic forms. A storage gestalt may also be memorized by the tabular format and you may memorize diagrammatically. Moreover, immediate memory may be carried out to the file of a calculating machine, and it does not matter even if it memorizes using a relational database, a directory server, etc.

[0031] Conversion to drawing 2 and the information illustrated to drawing 8 from the information illustrated to 3 and 7 which illustrated the algorithm by drawing 11 and 12 may be performed by the central policy DB1, and you may carry out by duplicate DB2. Moreover, management and a control unit 3 may perform. A database may be constituted only from a central policy DB1, and may consist of a central policy DB1 and duplicate DB2. The function of supervisory control equipment may be executed by proxy with the central policy DB or Duplicate DB, and supervisory control equipment may be omitted. The information generated from information, such as drawing 2, and 3, 7, may also include setting out of the arbitration about router control, and may reduce a labor in setting out of arbitration. For example, setting out of QoS may be generated, and as long as it is unnecessary, it may be omitted. As a candidate of the item set up, an access list, a path control method, an authentication method, a cipher system, QoS, etc. can be considered.

[0032] Moreover, although the approach of introducing software and constituting this invention from drawing 13 to a common computer was illustrated, the computer beforehand equipped with ROM which wrote in exclusive software may be used, or what hardware-ized the required part may be used. In addition, the above-mentioned software by which installation is carried out is introduced into each computer through magnetic-recording media, such as FD and CD-ROM, an optical recording medium, or the network connected to other servers.

[0033]

[Effect of the Invention] Network security and a network QoS function can be improved by offering the structure which sets up access list, QoS setting out, VPN setting out, etc. of a large-scale network simply while consisting of subnets in which many management policies differ from two or more routers or Firewall equipment according to this invention so that clearly in the above example, and setting up a network device correctly.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The example of a configuration of the network by this invention.
[Drawing 2] Example of a content of the central policy DB1 (Zone definition).
[Drawing 3] Example of a content of the central policy DB1 (AP definition).
[Drawing 4] The example of a content display of the central policy DB1 corresponding to the definition illustrated by drawing 2.
[Drawing 5] The example of a content display of the central policy DB1 corresponding to the definition illustrated by drawing 3.
[Drawing 6] The example of the content display classified by application of the central policy DB1.
[Drawing 7] The example of a definition of extra information.
[Drawing 8] The generated example of configuration information.
[Drawing 9] The example of the content of storage of supervisory control equipment 3.
[Drawing 10] The example of a data communication protocol.
[Drawing 11] The example of data flow of a configuration information generate time.
[Drawing 12] The example of an algorithm for configuration information generation.
[Drawing 13] The central policy DB1, duplicate DB2, and the example of a configuration of supervisory control equipment 3.
[Description of Notations]
1 [-- Administrative I/O device,] -- The central policy DB, 2 -- Duplicate DB, 3 -- Supervisory control equipment, 4 5 -- Intranet, 6 -- The Internet, 11, 12, 13, 14, 15, 16, 17 -- The content of storage of the central policy DB, 100 -- The example of the router definition inside central policy DB, 101 -- The example of the VPN definition inside central policy DB, 111 -- The Internet Zone definition inside central policy DB, 121 -- The FireWall Zone definition inside central policy DB, 131 -- The A place-of-business Zone definition inside central policy DB, 141 -- B place of business inside central policy DB Zone definition, 151 -- The accounting Zone definition inside central policy DB, 161 -- The labor Zone definition inside central policy DB, the application inside 171 -- central policy DB -- the definition of AP1, and the example of the data for router control inside 300 -- supervisory control equipment -- 301 -- The example of the data for VPN control inside supervisory control equipment, 302 -- The example of router setting out inside supervisory control equipment, 303 -- The example of VPN setting out inside supervisory control equipment, 52 -- Firewall, 531,541,537 [-- The computer of Accounting Zone, 536,546 / -- Computer of Labor Zone.] -- A router, 532, 533, 535,538,539,536 -- The computer of the A place of business Zone, 542,543,545,546 -- The computer of the B place of business Zone, 535,545

[Translation done.]

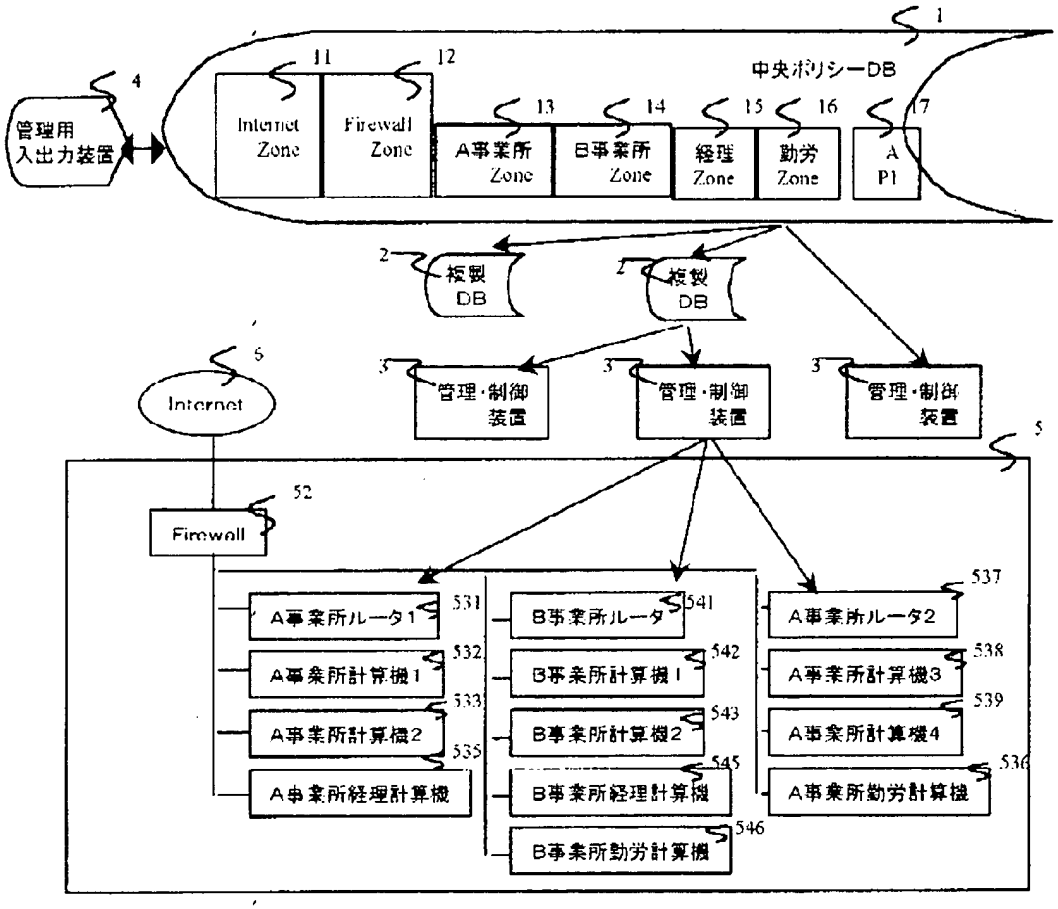
* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]

図1



[Drawing 3]

図3

171

ＡＰ１定義

アプリ名	実行計算機	通信先	ポート番号	優先度	
AP171	A事業所Zone	B事業所計算機１	1111	中	1711
		B事業所計算機２	1112		1712
AP172	A事業所計算機２	B事業所計算機２	1113		1713
		B事業所計算機１	1114		1714
		A事業所Zone	1115		1715

[Drawing 2]

図2

Internet Zone定義 111

アプリケーション種別	通信先	優先度	通信禁止	
電子mail	FireWall Zone	中		1111
news	FireWall Zone			1112
WWW	FireWall Zone			1113
telnet	FireWall Zone		FireWallZone以外全て	1114
上記以外全て			全て	1115

FireWall Zone定義 121

アプリケーション種別	通信先	優先度	通信禁止	
電子mail	全て	中		1211
news	全て			1212
WWW	Internet Zone			1213
WWW proxy	A, B事業所Zone			1214
telnet	全て			1215

A事業所Zone定義 131

アプリケーション種別	通信先	優先度	通信禁止	
電子mail	FireWall Zone	中		1311
news	FireWall Zone			1312
WWW proxy	FireWall Zone			1313
telnet	FireWall, B事業所Zone		Internet Zone	1314
4096	B事業所Zone	大	Internet Zone	1315
4097	B事業所Zone		Internet Zone	1316

B事業所Zone定義 141

アプリケーション種別	通信先	優先度	通信禁止	
電子mail	FireWall Zone	中		1411
news	FireWall Zone			1412
WWW proxy	FireWall Zone			1413
telnet	A事業所Zone		FireWall,Internet Zone	1414
4096	A事業所Zone	大	Internet Zone	1415
4097	A事業所Zone		Internet Zone	1416

経理Zone定義 151

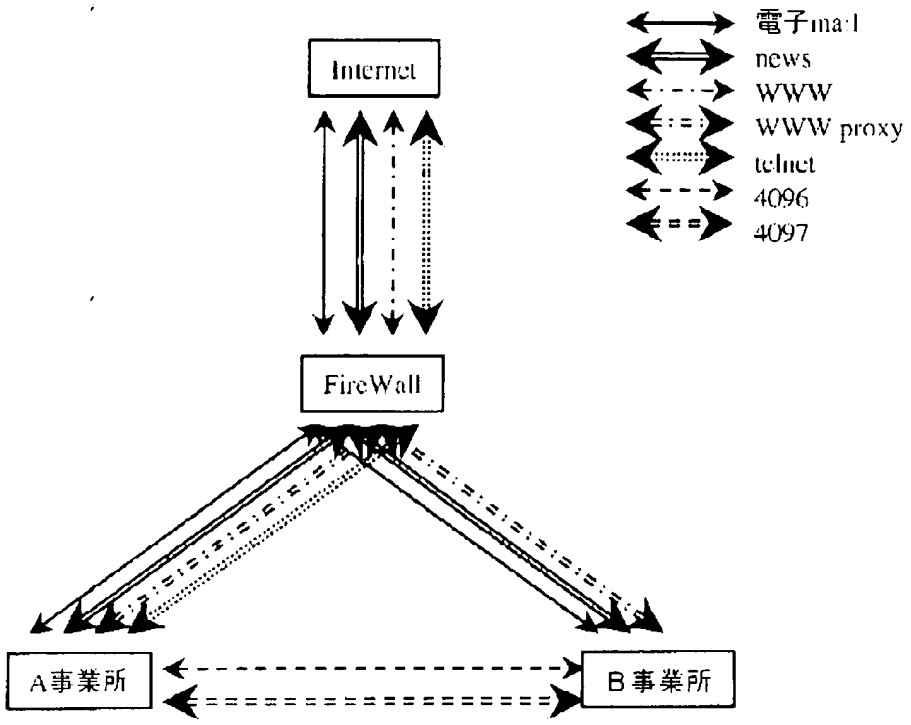
アプリケーション種別	通信先	優先度	通信禁止	
電子mail	経理Zoneのみ	中	経理以外禁止	1511
WWW proxy	経理Zoneのみ		経理以外禁止	1512
telnet	経理Zoneのみ		経理以外禁止	1513
5001	経理Zoneのみ	大	経理以外禁止	1514
5002	経理Zoneのみ		経理以外禁止	1515
5003	経理Zoneのみ		経理以外禁止	1516

勤労Zone定義 161

アプリケーション種別	通信先	優先度	通信禁止	
電子mail	勤労Zoneのみ	中	勤労以外禁止	1611
WWW proxy	勤労Zoneのみ		勤労以外禁止	1612
telnet	勤労Zoneのみ		勤労以外禁止	1613
5101	勤労Zoneのみ		勤労以外禁止	1614
5102	勤労Zoneのみ		勤労以外禁止	1615
5103	勤労Zoneのみ	大	勤労以外禁止	1616

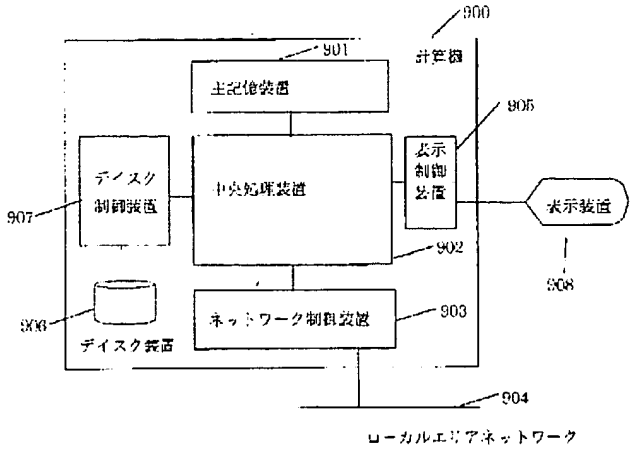
[Drawing 4]

図4



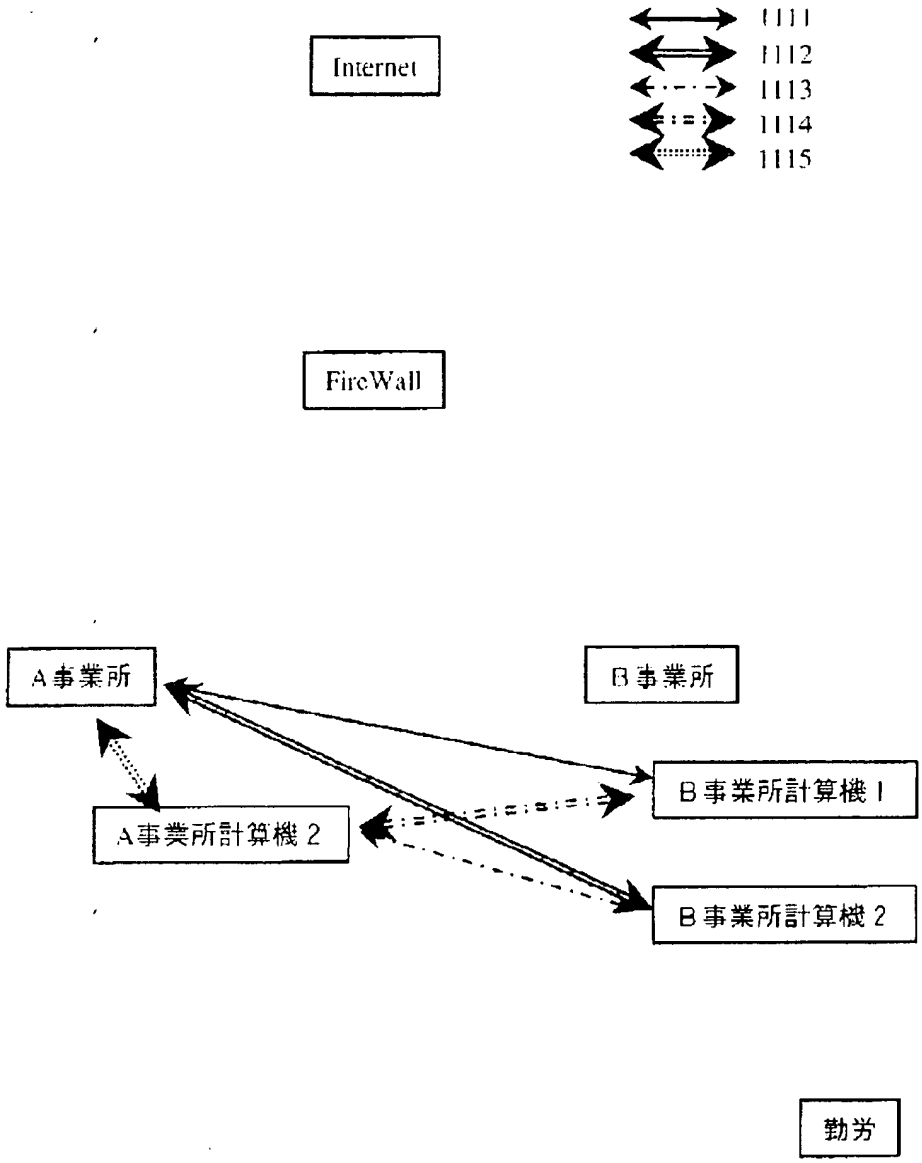
[Drawing 13]

図１３



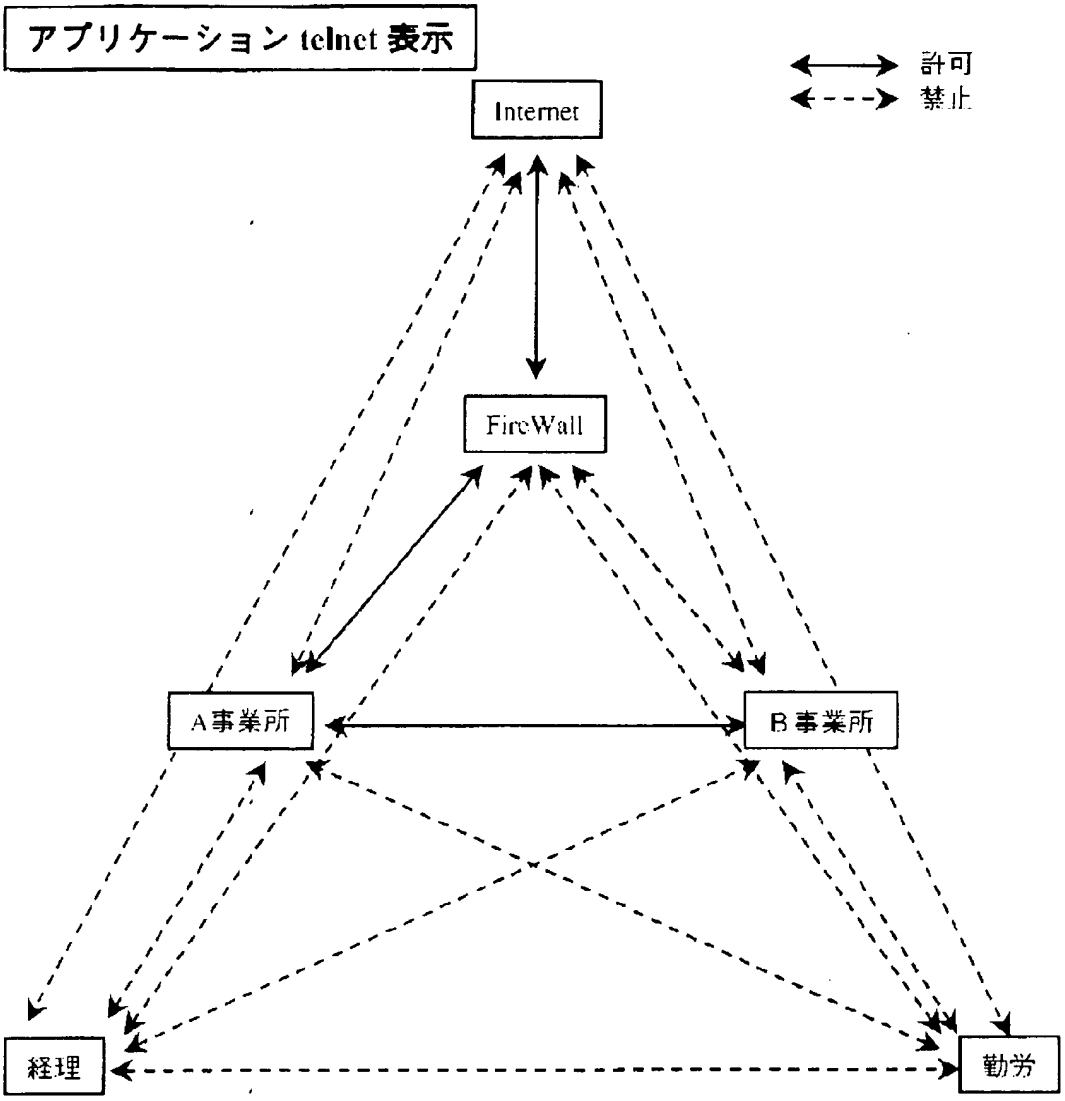
[Drawing 5]

図5



[Drawing 6]

図6



[Drawing 7]

図7

中間 ルータ 定義 100

設定項目	設定内容	
名称	router1	1001
ルータ初期化ファイル	X 1	1002
FireWall Zone インターフェース	192.10.0.1 (255.255.0.0)	1003
A事業所Zone インターフェース1	192.11.0.1 (255.255.0.0)	1004
B事業所Zone インターフェース	192.12.0.1 (255.255.0.0)	1005
A事業所Zone インターフェース2	192.13.0.1 (255.255.0.0)	1006

経理 ＶＰＮ 定義 （192.11.0.10用） 101

設定項目	設定内容	
名称	VPN1	1011
所属機械アドレス	192.11.0.10, 192.12.0.10	1012
初期化ファイル	X192.11.0.10, X192.12.0.10	1013
暗号化方式	Y1	1014
認証方式	Y2	1015
ポート番号	5000	1016

[Drawing 8]

図8

A事業所関連 ルータ 設定 (インターフェース1)

302

設定項目	設定内容	
インターフェースアドレス	192.11.0.1	3021
インターフェースアドレスマスク	255.255.0.0	
アクセス許可	ポート * 番：192.11.0.0 (255.255.0.0)	3022
アクセス許可	ポート 1111 番：192.12.10.1 (255.255.255.255)，優先度 2	3023
アクセス許可	ポート 1112 番：192.12.10.2 (255.255.255.255)	
アクセス許可	ポート 1113 番：192.12.10.2 (255.255.255.255),192.11.10.2	
アクセス許可	ポート 1114 番：192.12.10.1 (255.255.255.255),192.11.10.2	
アクセス不許可	ポート 23 番：not 192.0.0.0 (255.0.0.0)	3024
アクセス不許可	ポート 4096 番：not 192.0.0.0 (255.0.0.0)	
アクセス不許可	ポート 4097 番：not 192.0.0.0 (255.0.0.0)	3025
アクセス許可	ポート 5000 番：192.12.0.0 (255.255.0.0)，優先度 0	
アクセス許可	ポート 25 番：192.10.0.0 (255.255.0.0)，優先度 2	3026
アクセス許可	ポート 119 番：192.10.0.0 (255.255.0.0)，優先度 1	
アクセス許可	ポート 8080 番：192.10.0.0 (255.255.0.0)，優先度 1	
アクセス許可	ポート 23 番：192.10.0.0 (255.255.0.0)，優先度 1	
アクセス許可	ポート 23 番：192.12.0.0 (255.255.0.0)，優先度 1	
アクセス許可	ポート 4096 番：192.12.0.0 (255.255.0.0)，優先度 3	3027
アクセス許可	ポート 4097 番：192.12.0.0 (255.255.0.0)，優先度 1	
アクセス不許可	ポート * 番：0.0.0.0 (0.0.0.0)	3028

経理 VPN 設定 (192.11.0.10用)

303

設定項目	設定内容	
暗号化方式	Y1	3031
認証方式	Y2	3032
通信相手アドレス	192.12.0.10：5000	3033
アクセス許可	ポート 25 番：192.12.0.0 (255.255.0.0)，優先度 2	3034
アクセス許可	ポート8080 番：192.12.0.0 (255.255.0.0)，優先度 1	3035
アクセス許可	ポート 23 番：192.12.0.0 (255.255.0.0)，優先度 1	3036
アクセス許可	ポート5001 番：192.11.0.0 (255.255.0.0)，優先度 3	3037
アクセス許可	ポート5002 番：192.11.0.0 (255.255.0.0)，優先度 1	3038
アクセス許可	ポート5003 番：192.11.0.0 (255.255.0.0)，優先度 1	3039

[Drawing 9]

図9

中間ルータ用管理制御データ

300

設定項目	設定内容	
名称	router1	3001
ルータ初期化ファイル	X 1	3002
FireWall Zone インターフェース番号	00:20:AF:DF:87:9B	3003
A事業所Zone インターフェース番号 1	00:20:AF:DF:87:9C	3004
B事業所Zone インターフェース番号	00:20:AF:DF:87:9D	3005
A事業所Zone インターフェース番号 2	00:20:AF:DF:87:9E	3006
制御方式	Z 1	3007
制御用認証方式	Z 2	3008

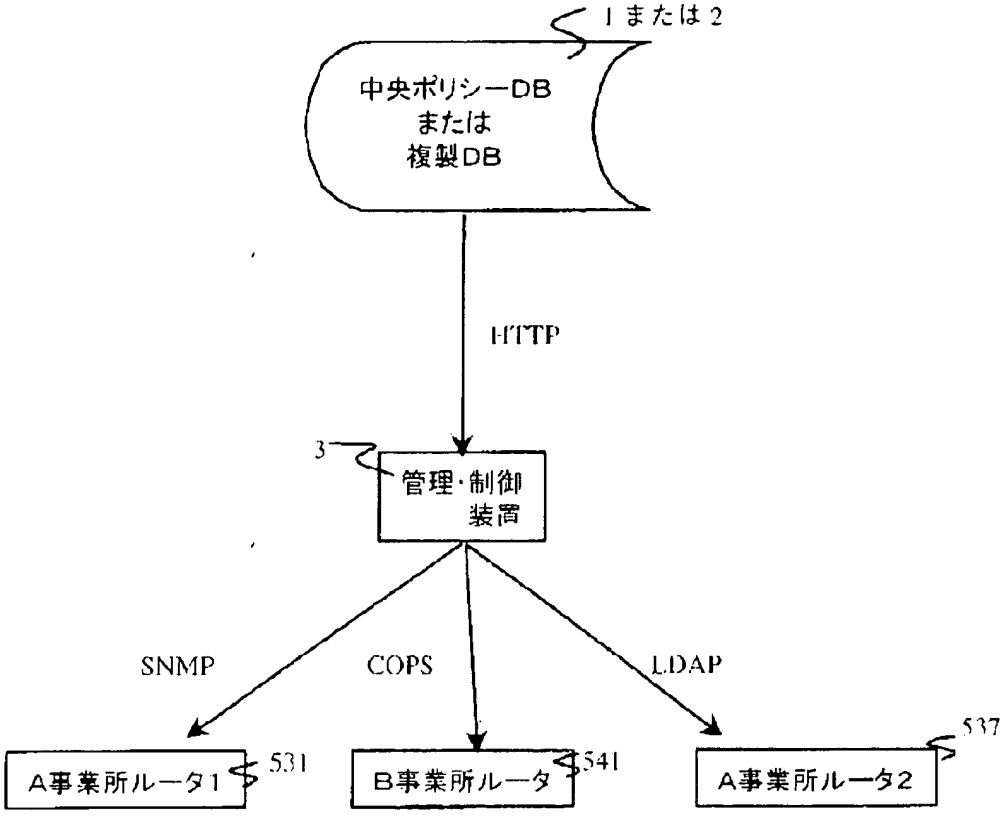
経理 VPN用管理制御データ (192.11.0.10用)

301

設定項目	設定内容	
名称	VPN1	3011
インターフェース番号	00:20:AF:DF:87:9A	3012
初期化ファイル	X192.11.0.10	3013
制御方式	Z 3	3014
制御用認証方式	Z 4	3015

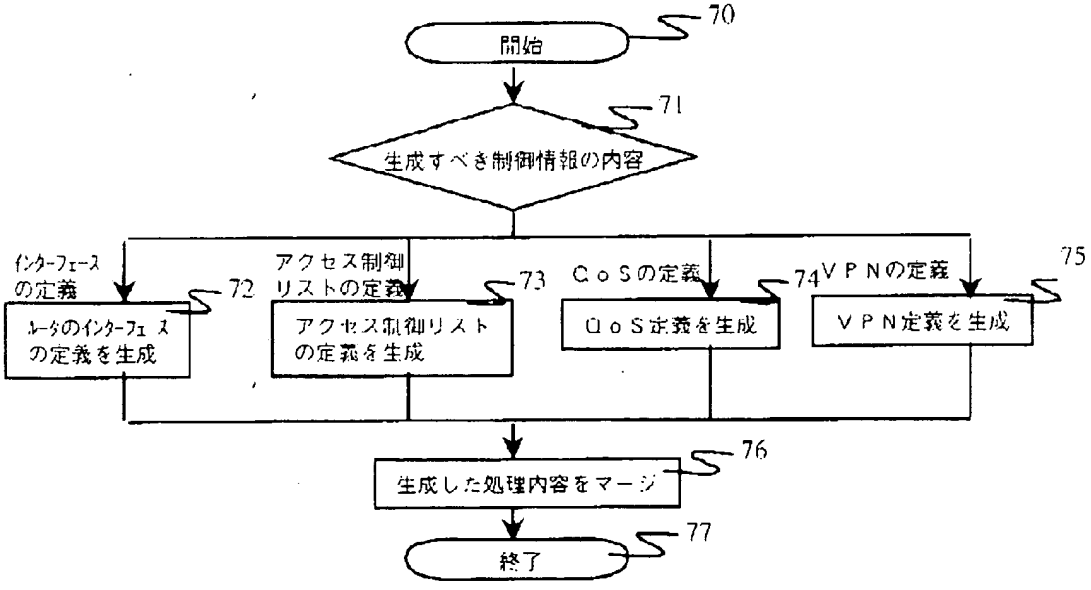
[Drawing 10]

図10



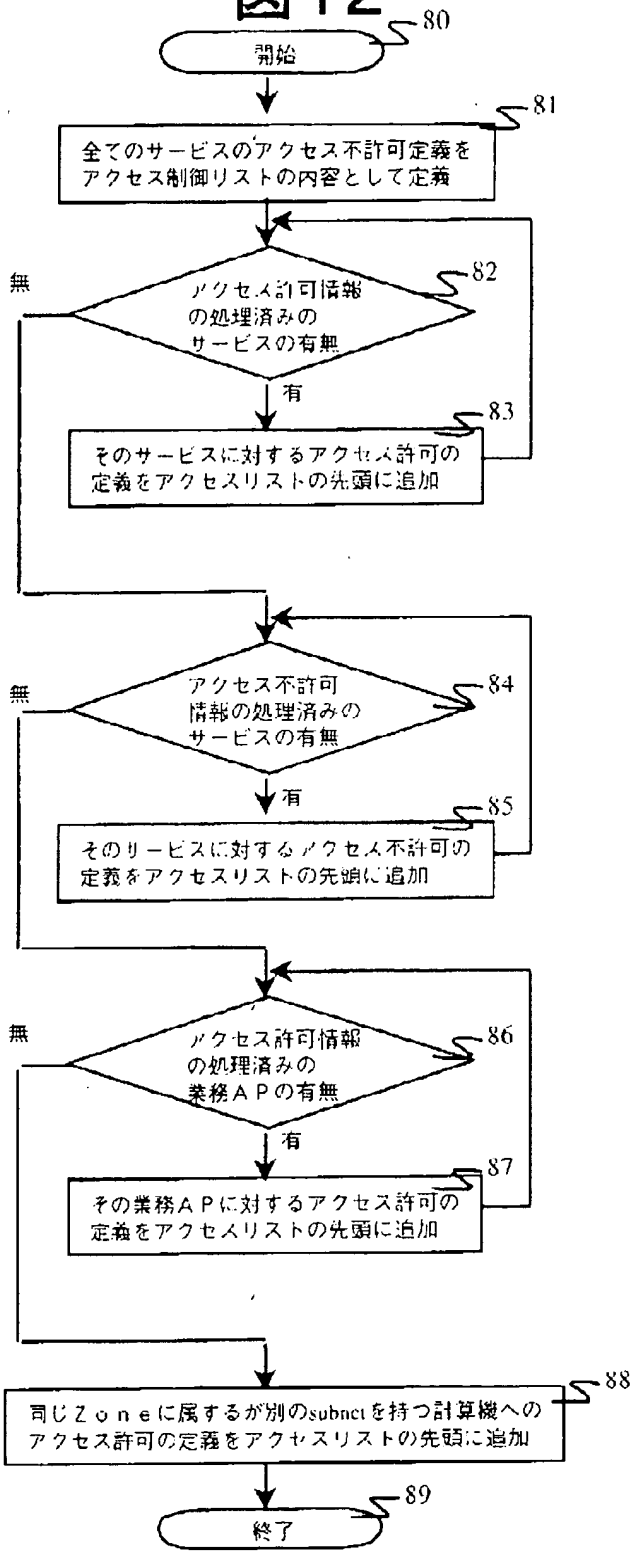
[Drawing 11]

図11



[Drawing 12]

図12



[Translation done.]